© 2019 IJSRSET | Volume 6 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology
DOI : 10.32628/IJSRSET196298

An Association-Based Graphical Password Design Resistant to Shoulder-Surfing Attack

Devi E[1], Kavi Bharathi K[1], Suruthy P[1], Keerthana S[2], Dr. Suguna N[3]
[1]UG students, [2]Assistant Professor, [3]Professor
Department of Computer Science and Engineering, Akshaya college of Engineering and technology, Coimbatore, Tamil Nadu, India

ABSTRACT

Data and computer protection is endured largely by countersigns which are the principle part of the authorization and authentication cognitive process. The most common information processing system authentication process is to apply alphanumerical username and password which has important drawbacks. Graphical passwords are often deliberated prone to shoulder-surfing attacks, where attackers can sneak a user's password by peeking over his or her shoulder in the certification process. Graphical passwords seem to be the solution as it is described more in the design structure of the authentication. A graphical password is an authentication scheme that works by accepting the user select from images, in a particular grade, demonstrated in a graphical user interface (GUI). The proposed research is an approach to enhance the subsisting Graphical Password techniques and resist against attacks like Shoulder Surfing. Based on the principle of zero-knowledge cogent evidence protocol, the additional improvement is the primary figure to overcome the shoulder-surfing attack issue without adding any additional complexity into the authentication process.

Keywords : GUI, zero-knowledge, Cogent Evidence Protocol, Graphical Password

I. INTRODUCTION

Generally, image processing is a method to convert an image into digital form and perform some operations on it, in order to get an enhanced image or extract some useful information from it. Image analysts use various fundamentals of interpretation while using these visual techniques. Digital image processing techniques help in manipulation of the digital images by using computers. The three general phases that all types of data have to undergo while using digital technique are pre-processing, enhancement, and display, information extraction. The textual passwords have been the most widely used authentication method for decades. Comprised of numbers and upper- and lower-case letters textual passwords are considered strong enough to resist against brute force attacks.

However, a strong textual password is hard to memorize and recollect. Therefore, users tend to choose passwords that are either short or from the dictionary, rather than random alphanumeric strings. Even worse, it is not a rare case that users may use only one user name and password for multiple accounts. According to an article in a computer world, a security team at a large company ran a network password cracker and surprisingly cracked approximately 80% of the employees' password within 30 seconds. Textual passwords are often insecure due to the difficulty of maintaining strong ones.

Various graphical passwords authentication schemes were developed to address the problems and weakness associated with textual passwords. Based on some studies such as those in humans have a better ability to memorize images with long term memory than verbal representations. Image-based passwords were proved to be easier to recollect in several user studies. As a result, users can set up a complex authentication password and are capable of recollecting it after a long time even if the memory is not activated periodically. However, most of these image-based passwords are vulnerable to shoulder surfing attacks.

This type of attack either uses direct observation, such as watching over someone's shoulder or applies video capturing techniques to get passwords, PINs, or other sensitive personal information.The human actions such as choosing bad passwords for new accounts and inputting passwords in an insecure way for later logins are regarded as the weakest link in the authentication chain. Therefore, an authentication scheme should be designed to overcome these vulnerabilities.

II. RELATED WORK

As a security measure, many banking websites display a security image and caption each time a user logs into account. When users first register for an account, they're prompted to pick a security image from a list of available images, and to create a caption to accompany the image. The user is presented with the security image and caption on all subsequent logins, and instructed not to log in if the image or caption is missing or incorrect. Despite the almost ubiquitous use of security images on banking sites, their effectiveness at preventing phishing attacks is uncertain. Even setting aside strategies that a sophisticated attacker might use to show the correct security image on a phishing site, we don't have a good understanding of users' ability to notice that an expected image is missing and then refuse to log in.

A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA). Graphical passwords are an alternative to alphanumeric passwords in which users click on images to authenticate rather than type alphanumeric strings. Graphical passwords are an alternative to alphanumeric passwords in which users click on images to authenticate rather than type alphanumeric strings. For providing security traditional authentication methods are used like credentials, OTP, LTP, etc. But there are major security threats while using this method. Web application and mobile application are used widely in everywhere with various devices.

For providing security traditional authentication methods are used like credentials, OTP, LTP, etc. But there are major security threats while using this method. Web application and mobile application are used widely in everywhere with various devices. This evolution is very useful but also increases probability leaking a password through shoulder surfing attacks. In this attack, attacker can observe directly or by external recording devices or video capturing are used for collecting password.

Computer security depends largely on passwords to authenticate human users. However, users have difficulty remembering passwords over time if they choose a secure password, i.e. a password that is long and random. Graphical passwords, which consist of clicking on images rather than typing alphanumeric strings, may help to overcome the problem of creating secure and memorable passwords. The participants subsequently carried out three longitudinal trials to input their password over the course of 6 weeks. The results show that the graphical password users created a valid password with fewer difficulties than the alphanumeric users. Graphical input devices enable the user to decouple the position of inputs from the

temporal order in which those inputs occur, and we show that this decoupling can be used to generate password schemes with substantially larger (memorable) password spaces.

In this work primarily motivated by devices such as personal digital assistants (PDAs) that or graphical input capabilities via a stylus, and describe our prototype implementation of one of our password schemes on such a PDA, namely the Palm Pilot. Security is the state of being free from danger or threat or errors. Computers and workstation, security is applied or measured through passwords. In our paper, a security Analysis of Graphical Passwords over the Textual Passwords through various schemes of graphical user authentication is analyzed. Here proposed graphical authentication scheme is implemented as an alternate to text-based authentication systems, various analyses are made and also several challenges in graphical authentication are discussed.

Users click on one point per image for a sequence of images. The next image is based on the previous click-point. present the results of an initial user study which revealed positive results. Performance was very good in terms of speed, accuracy, and number of errors. Also suggest that CCP provides greater security than Pass Points because the number of images increases the work load for attackers and have developed one such system, called Pass Points, and evaluated it with human users. The results of the evaluation were promising with respect to memorable of the graphical password.

III. SYSTEM MODEL

With the increasing amount of mobile devices and web services, users can access their personal accounts to send confidential business emails, upload photos to albums in the cloud or remit money from their e-bank account anytime and anywhere. While logging into these services in public, they may expose their password to unknown parties unconsciously. People with malicious intent could watch the whole authentication procedure through omnipresent video cameras and surveillance equipment, or even a reflected image on a window. Once the attacker obtains the password, they could access personal accounts and that would definitely pose a great threat to one's assets. Shoulder surfing attacks have gained more and more attention in the past decade.

- The problem of how to perform authentication in public so that shoulder surfing attacks can be alleviated.
- The problem of how to increase password space than that of the traditional PIN.
- The problem of how to efficiently search exact password objects during the authentication phase.
- The problem of requiring users to memorize extra information or to perform extra computation during authentication.
- The problem of limited usability of authentication schemes that can be applied to some devices only.

IV. PROPOSED SYSTEM

A graphical password is an authentication system that works by having the user select or drawing images, in a specific order, presented in a graphical user interface (GUI). Thus it is sometimes called graphical user authentication (GUA). A graphical user interface is a human-computer interface that uses windows, icons and menus and which can be manipulated by a mouse or a keyboard as well.

Password space plays an important role in achieving high security. Adequately larger number of pictures will cause bigger password space in graphical password models than in text based ones and therefore it makes the system virtually more immune to attacks like dictionary attacks but mostly there are no pre-existing dictionaries to search for graphical information. Still in few systems like click-based and image selection-based approach, password entropy

being small is an encountered problem that causes the whole method being weak against guessing attacks.

In our proposed primary authentication scheme, two levels of association are created – the association between the locus and the object, and the association between the object and its color. Byusing mnemonics technique similar to the Method of Loci, Alice could remember the associated locus, object and color as a "bundle", rather than separately. The associations are provided as follows, i) visualization must be conducted, no matter whether the user has witnessed the scene in real life. ii) The objects must be depicted in some kind of"interacting unity". Note that arbitrary associations may create some "bizarre scenes", Therefore, Alice is encouraged to create "bizarre scenes" to enhance the mnemonic effect.

Another great advantage of this strategy is that the password can be unbiasly distributed among users and thus the password entropy can be maintained. We argue that this association-based approach is superior compared to the recall-based approach, since associative memory is what the human is better at. On the other hand, it is superiorcompared to the recognition-based approach, because it leaves Alice much more choices of action to take, leading to much larger password entropy.

The principle of this protocol is: if Alice wants to prove to another verifier her knowledge of some secret information, but without revealing the secret's detail to the verifier, she can prove it by solving a "hard problem" – the "hard problem" is a special question that is easy to solve if the secret is known, and extremely hard if unknown. Therefore, by solving the problem, Alice can thereby prove her knowledge of that secret. Note that the "hard problem" must be carefully designed such that the verifier cannot get any information about the secret by observing Alice's solution.

The shoulder-surfing-resistant authentication involves a slightly different situation of the zero-knowledge proof protocol. The basic idea is that if Alice can prove to the MV that she knows some secret information but without revealing it during the process of proof, she can authenticate herself to the MV, and in the mean time, avoid revealing this information to the shoulder-surfer Bob.

Consider that Alice knows the pass color, so choosing the right subset is an easy job; however, since Bob does not know the pass color, he has no clue which subset to choose, but only can take his chance to guess. Note that this "hard problem" is not "perfect" because it is not fully secret-concealable – Bob still can get some information about the right pass color during the observation (i.e. narrowing down the possible pass colors to the subset selected by Alice).

We then measure the resistance to shoulder-surfing attack in terms of how many times Bob needs to observe Alice's authentication procedure, in order to interpret the correct password. The best case happens to Bob when in the second observation, for every round, the random clustering puts the pass color in a totally different subset without any overlapping decoy colors as in the first observation. In this case, Bob needs to observe twice to interpret the right password; in the worst case, however, when there are always overlapping decoy colors, it takes infinite observations for Bob to discover the password.

Based on the size of userid, password and domain parameters the keysize is decided. The size of security parameters[userid, password and domain parameters] is inversely proportional to the keysize[i,e password being small it is possible to hacked using brute force attack].

(i) To overcome the vulnerability issues,large keysize is assigned to small passwords.

(ii) If password length being large, the decryption time is large. To resolve this keysize and padding length is reduced in proposed approach.

In the system, during login, system will compute the formula in background according to the login screen and will provide result in"token" form. Now user will take the value of every character of his textual password from the login screen and integrate it with the "token" by using the set of operators to generate the resultant login value, the resultant value from the integration will be the login value. It involves two type of process, recalling the textual password and integrates it with the token. Instead of entering the original password, result is got entered. This technique provides strong resistant against shoulder surfmg, dictionary attacks, bruteforce attack.

V. CONCLUSION

Using traditional textual passwords or PIN method, users need to type their passwords to authenticate and these passwords can be revealed easily if someone peeks over shoulder or uses video recording devices such as cell phones. Based on the results, Pass Matrix is a novel and easy to use graphical password authentication system can effectively alleviate shoulder surfing attacks. In addition, Pass Matrix can be applied to any authentication scenario and device with simple input and output capabilities. Future research will concentrate to improving YAGP and developing a comparison algorithm of higher efficiency in distinguishing the legal user from attackers.

VI. REFERENCES

[1]. J. Kirk, “Study: Users ignore bank security features,” Computerworld, Feb. 2007,

[2]. http://www.computerworld.com/s/article/9010283 /Study_Users_ignore_ bank_security_features_.

[3]. Bank of America, “SiteKey FAQs,” https://www.bankofamerica.com/privacy/faq/sitekey-faq.go, 2013.

[4]. PNC, “Online security information,” https://www.pnc.com/webapp/unsec/Solutions.do ?siteArea=/pnccorp/PNC/ security+Information/Security+Information, 2013.

[5]. Santander Bank, “SSA makes online banking even more secure,” https://www.santanderbank.com/us/personal/banking/online-andmobile- banking/security-center/ssa-learn-more, 2014.

[6]. S. Schechter, R. Dhamija, A. Ozment, and I. Fischer, “The emperor’s new security indicators: An evaluation of website authentication and the effect of role playing on usability studies,” in Proceedings of the 28th IEEE Symposium on Security and Privacy, 2007.

[7]. Herzberg and R. Margulies, “Forcing Johnny to login safely,” in Proceedings of the 16th European Symposium on Research in Computer Security, 2011.

[8]. M. Wu, R. C. Miller, and S. L. Garfinkel, “Do security toolbars actually prevent phishing attacks?” in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2010.

[9]. J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor, “Crying wolf: An empirical study of SSL warning effectiveness,” in Proceedings of the 18th USENIX Security Symposium, 2009.

[10]. “U.S. patent number 5,559,961,” 1996.

[11]. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, “The design and analysis of graphical passwords,” in Proceedings of the 8th USENIX Security Symposium, 1999.

Cite this article as :

Devi E, Kavi Bharathi K, Suruthy P, Keerthana S, Dr. Suguna N" An Association-Based Graphical Password Design Resistant to Shoulder-Surfing Attack, International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 6, Issue 2, pp.324-328, March-April-2019.

Journal URL : http://ijsrset.com/IJSRSET196298